



Cisco TrustSec Commands

- [cts authorization list, on page 3](#)
- [cts change-password, on page 4](#)
- [cts credentials, on page 5](#)
- [cts refresh, on page 7](#)
- [cts rekey, on page 9](#)
- [cts role-based enforcement, on page 10](#)
- [cts role-based l2-vrf, on page 11](#)
- [cts role-based monitor, on page 13](#)
- [cts role-based permissions, on page 14](#)
- [cts role-based sgt-caching, on page 16](#)
- [cts role-based sgt-map, on page 17](#)
- [cts sxp connection peer, on page 19](#)
- [cts sxp default password, on page 22](#)
- [cts sxp default source-ip, on page 24](#)
- [cts sxp filter-enable, on page 26](#)
- [cts sxp filter-group, on page 27](#)
- [cts sxp filter-list, on page 29](#)
- [cts sxp log binding-changes, on page 31](#)
- [cts sxp reconciliation period, on page 32](#)
- [cts sxp retry period, on page 33](#)
- [propagate sgt \(cts manual\), on page 34](#)
- [sap mode-list \(cts manual\), on page 36](#)
- [show cts credentials, on page 38](#)
- [show cts interface, on page 39](#)
- [show cts role-based counters, on page 41](#)
- [show cts role-based permissions, on page 43](#)
- [show cts server-list, on page 45](#)
- [show cts sxp, on page 47](#)
- [show platform hardware fed switch active fwd-asic resource team utilization , on page 50](#)
- [show platform hardware fed switch active sgacl resource usage, on page 52](#)
- [show platform software classification switch active F0 class-group-manager class-group client acl all, on page 53](#)
- [show platform software cts forwarding-manager switch active F0 port, on page 54](#)

- [show platform software cts forwarding-manager switch active F0](#), on page 58
- [show platform software cts forwarding-manager switch active F0 permissions](#), on page 59
- [show platform software fed switch active acl counters hardware | inc SGACL](#) , on page 60
- [show platform software fed switch active acl usage](#) , on page 61
- [show platform software fed switch active ifm mappings](#) , on page 62
- [show platform software fed switch active ip route](#) , on page 64
- [show platform software fed switch active sgacl detail](#) , on page 66
- [show platform software fed switch active sgacl port](#) , on page 67
- [show platform software fed switch active sgacl vlan](#) , on page 69
- [show platform software status control-processor brief](#), on page 70

cts authorization list

To specify a list of authentication, authorization, and accounting (AAA) servers to be used by the TrustSec seed device, use the **cts authorization list** command on the Cisco TrustSec seed device in global configuration mode. Use the **no** form of the command to stop using the list during authentication.

cts authorization list *server_list*

no cts authorization list *server_list*

Syntax Description *server_list* Cisco TrustSec AAA server group.

Command Default None

Command Modes Global configuration (config)

Supported User Roles

Administrator

| Command History | Release | Modification |
|-----------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines This command is only for the seed device. Non-seed devices obtain the TrustSec AAA server list from their TrustSec authenticator peer as a component of their TrustSec environment data.

The following example displays an AAA configuration of a TrustSec seed device:

```
Device# cts credentials id Device1 password Cisco123
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
Device(config)# aaa authorization network MLIST group radius
Device(config)# cts authorization list MLIST
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key
AbCe1234
Device(config)# radius-server vsa send authentication
Device(config)# dot1x system-auth-control
Device(config)# exit
```

| Related Commands | Command | Description |
|------------------|-----------------------------|--|
| | show cts server-list | Displays RADIUS server configurations. |

cts change-password

To change the password between the local device and the authentication server, use the **cts change-password** privileged EXEC command.

```
cts change-password server ipv4_address udp_port {a-id hex_string | key radius_key }[{source interface_list}]
```

Syntax Description

| | |
|-------------------------------------|---|
| server | Specifies the authentication server. |
| <i>ipv4_address</i> | IP address of the authentication server. |
| <i>udp_port</i> | UPD port of the authentication server. |
| a-id <i>hex_string</i> | Specifies the identification string of the ACS server. |
| key | Specifies the RADIUS key to be used for provisioning. |
| source <i>interface_list</i> | (Optional) Specifies the interface type and its identifying parameters as per the displayed list for source address in request packets. |

Command Default

None.

Command Modes

Privileged EXEC (#)

Supported User Roles

Administrator

Command History

| Release | Modification |
|--------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines

The **cts change-password** command allows an administrator to change the password used between the local device and the Cisco Secure ACS authentication server, without having to reconfigure the authentication server.

The following example shows how to change the Cisco TrustSec password between a switch and a Cisco Secure ACS:

```
Device# cts change-password server 192.168.2.2 88 a-id ffe
```

cts credentials

Use the **cts credentials** command in privileged EXEC mode to specify the TrustSec ID and password of the network device. Use the **clear cts credentials** command to delete the credentials.

```
cts credentials id cts_id password cts_pwd
```

| Syntax Description | |
|-------------------------------------|--|
| credentials id <i>cts_id</i> | Specifies the Cisco TrustSec device ID for this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The <i>cts-id</i> variable has a maximum length of 32 characters and is case sensitive. |
| password <i>cts_pwd</i> | Specifies the password for this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST. |

Command Default None

Command Modes Privileged EXEC (#)

Supported User Roles

Administrator

| Command History | Release | Modification |
|-----------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines The **cts credentials** command specifies the Cisco TrustSec device ID and password for this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The Cisco TrustSec credentials state retrieval is not performed by the nonvolatile generation process (NVGEN) because the Cisco TrustSec credential information is saved in the keystore, and not in the startup configuration. The device can be assigned a Cisco TrustSec identity by the Cisco Secure Access Control Server (ACS), or a new password auto-generated when prompted to do so by the ACS. These credentials are stored in the keystore, eliminating the need to save the running configuration. To display the Cisco TrustSec device ID, use the **show cts credentials** command. The stored password is never displayed.

To change the device ID or the password, reenter the command. To clear the keystore, use the **clear cts credentials** command.



Note When the Cisco TrustSec device ID is changed, all Protected Access Credentials (PACs) are flushed from the keystore because PACs are associated with the old device ID and are not valid for a new identity.

The following example shows how to configure the Cisco TrustSec device ID and password:

```
Device# cts credentials id cts1 password password1
CTS device ID and password have been inserted in the local keystore. Please make sure that
the same ID and password are configured in the server database.
```

The following example show how to change the Cisco TrustSec device ID and password to cts_new and password123, respectively:

```
Device# cts credentials id cts_new password password123
A different device ID is being configured.
This may disrupt connectivity on your CTS links.
Are you sure you want to change the Device ID? [confirm] y
```

TS device ID and password have been inserted in the local keystore. Please make sure that the same ID and password are configured in the server database.

The following sample output displays the Cisco TrustSec device ID and password state:

```
Device# show cts credentials

CTS password is defined in keystore, device-id = cts_new
```

Related Commands

| Command | Description |
|------------------------------|--|
| clear cts credentials | Clears the Cisco TrustSec device ID and password. |
| show cts credentials | Displays the state of the current Cisco TrustSec device ID and password. |
| show cts keystore | Displays contents of the hardware and software keystores. |

cts refresh

To refresh the TrustSec peer authorization policy of all or specific Cisco TrustSec peers, or to refresh the SGACL policies downloaded to the device by the authentication server, use the **cts refresh** command in privileged EXEC mode.

```
cts refresh {peer [peer_id] | sgt [{sgt_number | default | unknown}]}
```

Syntax Description

| | |
|------------------------------|---|
| environment-data | Refreshes environment data. |
| peer <i>Peer-ID</i> | (Optional) If a peer-id is specified, only policies related to the specified peer connection are refreshed. |
| sgt <i>sgt_number</i> | (Optional) Performs an immediate refresh of the SGACL policies from the authentication server. If an SGT number is specified, only policies related to that SGT are refreshed. |
| default | (Optional) Refreshes the default SGACL policy. |
| unknown | (Optional) Refreshes the unknown SGACL policy. |

Command Default

None

Command Modes

Privileged EXEC (#)

Supported User Roles

Administrator

Command History

| Release | Modification |
|--------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines

To refresh the Peer Authorization Policy on all TrustSec peers, enter **cts policy refresh** without specifying a peer ID.

The peer authorization policy is initially downloaded from the Cisco ACS at the end of the EAP-FAST NDAC authentication success. The Cisco ACS is configured to refresh the peer authorization policy, but the **cts policy refresh** command can force immediate refresh of the policy before the Cisco ACS timer expires. This command is relevant only to TrustSec devices that can impose Security Group Tags (SGTs) and enforce Security Group Access Control Lists (SGACLs).

The following example shows how to refresh the TrustSec peer authorization policy of all peers:

```
Device# cts policy refresh
Policy refresh in progress
```

The following sample output displays the TrustSec peer authorization policy of all peers:

```
VSS-1# show cts policy peer
```

```

CTS Peer Policy
=====
device-id of the peer that this local device is connected to
Peer name: VSS-2T-1
Peer SGT: 1-02
Trusted Peer: TRUE
Peer Policy Lifetime = 120 secs
Peer Last update time = 12:19:09 UTC Wed Nov 18 2009
Policy expires in 0:00:01:51 (dd:hr:mm:sec)
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)
Cache data applied = NONE

```

Related Commands

| Command | Description |
|-----------------------------|--|
| clear cts policy | Clears all Cisco TrustSec policies, or by the peer ID or SGT. |
| show cts policy peer | Displays peer authorization policy for all or specific TrustSec peers. |

cts rekey

To regenerate the Pairwise Master Key used by the Security Association Protocol (SAP), use the **cts rekey** privileged EXEC command.

cts rekey interface type slot/port

Syntax Description

interface type slot/port Specifies the Cisco TrustSec interface on which to regenerate the SAP key.

Command Default

None.

Command Modes

Privileged EXEC (#)

Supported User Roles

Administrator

Command History

Release

Cisco IOS XE Fuji 16.9.1

Modification

This command was introduced.

Usage Guidelines

SAP Pair-wise Master Key key (PMK) refresh ordinarily occurs automatically, triggered by combinations of network events and non-configurable internal timers related to dot1X authentication. The ability to manually refresh encryption keys is often part of network administration security requirements. To manually force a PMK refresh, use the **cts rekey** command.

TrustSec supports a manual configuration mode where dot1X authentication is not required to create link-to-link encryption between switches. In this case, the PMK is manually configured on devices on both ends of the link with the **sap pmk** Cisco TrustSec manual interface configuration command.

The following example shows how to regenerate the PMK on a specified interface:

```
Device# cts rekey interface gigabitEthernet 2/1
```

Related Commands

| Command | Description |
|-----------------------------------|--|
| sap mode-list (cts manual) | Configures Cisco TrustSec SAP for manual mode. |

cts role-based enforcement

To enable role-based access control globally and on specific Layer 3 interfaces using Cisco TrustSec, use the **cts role-based enforcement** command in global configuration mode and interface configuration mode respectively. To disable the enforcement of role-based access control at an interface level, use the **no** form of this command.

cts role-based enforcement
no cts role-based enforcement

Syntax Description

This command has no keywords or arguments.

Command Default

Enforcement of role-based access control at an interface level is disabled globally.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

| Release | Modification |
|--------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines

The **cts role-based enforcement** command in global configuration mode enables role-based access control globally. Once role-based access control is enabled globally, it is automatically enabled on every Layer 3 interface on the device. To disable role-based access control on specific Layer 3 interfaces, use the **no** form of the command in interface configuration mode. The **cts role-based enforcement** command in interface configuration mode enables enforcement of role-based access control on specific Layer 3 interfaces.

The attribute-based access control list organizes and manages the Cisco TrustSec access control on a network device. The security group access control list (SGACL) is a Layer 3-4 access control list to filter access based on the value of the security group tag (SGT). The filtering usually occurs at an egress port of the Cisco TrustSec domain. The terms role-based access control list (RBACL) and SGACL can be used interchangeably, and they refer to a topology-independent ACL used in an attribute-based access control (ABAC) policy model.

The following example shows how to enable role-based access control on a Gigabit Ethernet interface:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/3
Device(config-if)# cts role-based enforcement
Device(config-if)# end
```

cts role-based l2-vrf

To select a virtual routing and forwarding (VRF) instance for Layer 2 VLANs, use the **cts role-based l2-vrf** command in global configuration mode. To remove the configuration, use the **no** form of this command.

```
cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [{,}] [{-}]
no cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [{,}] [{-}]
```

Syntax Description

| | |
|------------------|---|
| <i>vrf-name</i> | Name of the VRF instance. |
| vlan-list | Specifies the list of VLANs to be assigned to a VRF instance. |
| all | Specifies all VLANs. |
| <i>vlan-ID</i> | VLAN ID. Valid values are from 1 to 4094. |
| , | (Optional) Specifies another VLAN separated by a comma. |
| - | (Optional) Specifies a range of VLANs separated by a hyphen. |

Command Default

VRF instances are not selected.

Command Modes

Global configuration (config)

Command History

| Release | Modification |
|--------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines

The *vlan-list* argument can be a single VLAN ID, a list of comma-separated VLAN IDs, or hyphen-separated VLAN ID ranges.

The **all** keyword is equivalent to the full range of VLANs supported by the network device. The **all** keyword is not preserved in the nonvolatile generation (NVGEN) process.

If the **cts role-based l2-vrf** command is issued more than once for the same VRF, each successive command entered adds the VLAN IDs to the specified VRF.

The VRF assignments configured by the **cts role-based l2-vrf** command are active as long as a VLAN remains a Layer 2 VLAN. The IP-SGT bindings learned while a VRF assignment is active are also added to the Forwarding Information Base (FIB) table associated with the VRF and the IP protocol version. If an Switched Virtual Interface (SVI) becomes active for a VLAN, the VRF-to-VLAN assignment becomes inactive and all bindings learned on the VLAN are moved to the FIB table associated with the VRF of the SVI.

Use the **interface vlan** command to configure an SVI interface, and the **vrf forwarding** command to associate a VRF instance to the interface.

The VRF-to-VLAN assignment is retained even when the assignment becomes inactive. It is reactivated when the SVI is removed or when the SVI IP address is changed. When reactivated, the IP-SGT bindings are moved back from the FIB table associated with the VRF of the SVI to the FIB table associated with the VRF assigned by the **cts role-based l2-vrf** command.

The following example shows how to select a list of VLANs to be assigned to a VRF instance:

```
Device(config)# cts role-based l2-vrf vrf1 vlan-list 20
```

The following example shows how to configure an SVI interface and associate a VRF instance:

```
Device(config)# interface vlan 101
Device(config-if)# vrf forwarding vrf1
```

Related Commands

| Command | Description |
|--|---|
| interface vlan | Configures a VLAN interface. |
| vrf forwarding | Associates a VRF instance or a virtual network with an interface or subinterface. |
| show cts role-based permissions | Displays the SGACL permission list. |

cts role-based monitor

To enable role-based (security-group) access list monitoring, use the **cts role-based monitor** command in global configuration mode. To remove role-based access list monitoring, use the **no** form of this command.

```
cts role-based monitor {all | permissions {default [{ipv4 | ipv6}] | from {sgt | unknown} to {sgt
| unknown} [{ipv4 | ipv6}]}}
no cts role-based monitor {all | permissions {default [{ipv4 | ipv6}] | from {sgt | unknown} to {sgt
| unknown} [{ipv4 | ipv6}]}}
```

Syntax Description

| | |
|--------------------|---|
| all | Monitors permissions for all source tags to all destination tags. |
| permissions | Monitors permissions from a source tags to a destination tags. |
| default | Monitors the default permission list. |
| ipv4 | (Optional) Specifies the IPv4 protocol. |
| ipv6 | (Optional) Specifies the IPv6 protocol. |
| from | Specifies the source group tag for filtered traffic. |
| <i>sgt</i> | Security Group Tag (SGT). Valid values are from 2 to 65519. |
| unknown | Specifies an unknown source or destination group tag (DST). |

Command Default

Role-based access control monitoring is not enabled.

Command Modes

Global configuration (config)

Command History

| Release | Modification |
|-----------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines

Use the **cts role-based monitor all** command to enable the global monitor mode. If the **cts role-based monitor all** command is configured, the output of the **show cts role-based permissions** command displays monitor mode for all configured policies as true.

The following examples shows how to configure SGACL monitor from a source tag to a destination tag:

```
Device(config)# cts role-based monitor permissions from 10 to 11
```

Related Commands

| Command | Description |
|--|-------------------------------------|
| show cts role-based permissions | Displays the SGACL permission list. |

cts role-based permissions

To enable permissions from a source group to a destination group, use the **cts role-based permissions** command in global configuration mode. To remove the permissions, use the **no** form of this command.

```
cts role-based permissions {default | from {sgt | unknown} to {sgt | unknown}} {rbacl-name | ipv4 | ipv6}
no cts role-based permissions {default | from {sgt | unknown} to {sgt | unknown}} {rbacl-name | ipv4 | ipv6}
```

| Syntax Description | | |
|--------------------|---|--|
| default | Specifies the default permissions list. Every cell (an SGT pair) for which, security group access control list (SGACL) permission is not configured statically or dynamically falls under the default category. | |
| from | Specifies the source group tag of the filtered traffic. | |
| <i>sgt</i> | Security Group Tag (SGT). Valid values are from 2 to 65519. | |
| unknown | Specifies an unknown source or destination group tag. | |
| <i>rbacl-name</i> | Role-based access control list (RBACL) or SGACL name. Up to 16 SGACLs can be specified in the configuration. | |
| ipv4 | Specifies the IPv4 protocol. | |
| ipv6 | Specifies the IPv6 protocol. | |

Command Default Permissions from a source group to a destination group is not enabled.

Command Modes Global configuration (config)

| Command History | Release | Modification |
|-----------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines Use the **cts role-based permissions** command to define, replace, or delete the list of SGACLs for a given source group tag (SGT), destination group tag (DGT) pair. This policy is in effect as long as there is no dynamic policy for the same DGT or SGT.

The **cts role-based permissions default** command defines, replaces, or deletes the list of SGACLs of the default policy as long as there is no dynamic policy for the same DGT.

The following example shows how to enable permissions for a destination group:

```
Device(config)# cts role-based permissions from 6 to 6 mon_2
```

Related Commands

| Command | Description |
|--|-------------------------------------|
| show cts role-based permissions | Displays the SGACL permission list. |

cts role-based sgt-caching

To enable Security Group Tag (SGT) caching globally, use the **cts role-based sgt-caching** command in global configuration mode. To remove SGT caching, use the **no** form of this command.

```
cts role-based sgt-caching [vlan-list {vlan-id | all}]
no cts role-based sgt-caching [vlan-list {vlan-id | all}]
```

| Syntax Description | | |
|--------------------|---------------------------------|--|
| | vlan-list <i>vlan-id</i> | (Optional) Specifies VLAN IDs. Individual VLAN IDs are separated by commas, and a range of IDs specified with a hyphen. Valid values are from 1 to 4094. |
| | all | (Optional) Selects all VLANs. |

Command Default SGT caching is not configured.

Command Modes Global configuration (config)

| Command History | Release | Modification |
|-----------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines To enable SGT caching on a VLAN, both **cts role-based sgt-caching** and **cts role-based sgt-caching vlan-list** commands must be configured.

Example

The following example shows how to enable SGT caching on a VLAN:

```
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# cts role-based sgt-caching vlan-list 4
```


cts role-based sgt-map

To manually map a source IP address to a Security Group Tag (SGT) on either a host or a VRF, use the **cts role-based sgt-map** command in global configuration mode. Use the **no** form of the command to remove the mapping.

cts role-based sgt-map {*ipv4_netaddress* | *ipv6_netaddress* | *ipv4_netaddress/prefix* | *ipv6_netaddress/prefix*}
sgt *sgt-number*

cts role-based sgt-map host {*ipv4_hostaddress* | *ipv6_hostaddress*} **sgt** *sgt-number*

cts role-based sgt-map vlan-list [{*vlan_ids* | **all**}] **sgt** *sgt-number*

cts role-based sgt-map vrf *instance_name*

{*ipv4_netaddress* | *ipv6_netaddress* | *ipv4_netaddress/prefix* | *ipv6_netaddress/prefix*} **host**

{*ipv4_hostaddress* | *ipv6_hostaddress*} **sgt** *sgt-number*

no cts role-based sgt-map

Syntax Description

| | |
|--|--|
| <i>ipv4_netaddress</i> <i>ipv6_netaddress</i> | Specifies the network to be associated with an SGT. Enter IPv4 address in dot decimal notation; IPv6 in colon hexadecimal notation. |
| <i>ipv4_netaddress/prefix</i> <i>ipv6_netaddress/prefix</i> | Maps the SGT to all hosts of the specified subnet address (IPv4 or IPv6). IPv4 is specified in dot decimal CIDR notation, IPv6 in colon hexadecimal notation |
| host { <i>ipv4_hostaddress</i> <i>ipv6_hostaddress</i> } | Binds the specified host IP address with the SGT. Enter the IPv4 address in dot decimal notation; IPv6 in colon hexadecimal notation. |
| vlan-list { <i>vlan_ids</i> all } | Specifies VLAN IDs. <ul style="list-style-type: none"> • (Optional) <i>vlan_ids</i>: Individual VLAN IDs are separated by commas, a range of IDs specified with a hyphen. • (Optional) all: Specifies all VLAN IDs. |
| vrf <i>instance_name</i> | Specifies a VRF instance, previously created on the device. |
| sgt <i>sgt-number</i> | Specifies the SGT number from 0 to 65,535. |

Command Default

None

Command Modes

Global configuration (config)

Command History

| Release | Modification |
|-----------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines

If you do not have a Cisco Identity Services Engine, Cisco Secure ACS, dynamic Address Resolution Protocol (ARP) inspection, Dynamic Host Control Protocol (DHCP) snooping, or Host Tracking available on your

device to automatically map SGTs to source IP addresses, you can manually map an SGT to the following with the **cts role-based sgt-map** command:

- A single host IPv4 or IPv6 address
- All hosts of an IPv4 or IPv6 network or subnetwork
- VRFs
- Single or multiple VLANs

The **cts role-based sgt-map** command binds the specified SGT with packets that fall within the specified network address.

SXP exports an exhaustive expansion of all possible individual IP-SGT bindings within the specified network or subnetwork. IPv6 bindings and subnet bindings are exported only to SXP listener peers of SXP version 2 or later. The expansion does not include host bindings which are known individually or are configured or learnt from SXP for any nested subnet bindings.

The **cts role-based sgt-map host** command binds the specified SGT with incoming packets when the IP source address is matched by the specified host address. This IP-SGT binding has the lowest priority and is ignored in the presence of any other dynamically discovered bindings from other sources (such as, SXP or locally authenticated hosts). The binding is used locally on the device for SGT imposition and SGACL enforcement. It is exported to SXP peers if it is the only binding known for the specified host IP address.

The **vrf** keyword specifies a virtual routing and forwarding table previously defined with the vrf definition global configuration command. The IP-SGT binding specified with the **cts role-based sgt-map vrf** global configuration command is entered into the IP-SGT table associated with the specified VRF and the IP protocol version which is implied by the type of IP address entered.

The **cts role-based sgt-map vlan-list** command binds an SGT with a specified VLAN or a set of VLANs. The keyword **all** is equivalent to the full range of VLANs supported by the device and is not preserved in the nonvolatile generation (NVGEN) process. The specified SGT is bound to incoming packets received in any of the specified VLANs. The system uses discovery methods such as DHCP and/or ARP snooping (a.k.a. IP device tracking) to discover active hosts in any of the VLANs mapped by this command. Alternatively, the system could map the subnet associated with the SVI of each VLAN to the specified SGT. SXP exports the resulting bindings as appropriate for the type of binding.

Examples

The following example shows how to manually map a source IP address to an SGT:

```
Device(config)# cts role-based sgt-map 10.10.1.1 sgt 77
```

In the following example, a device binds host IP address 10.1.2.1 to SGT 3 and 10.1.2.2 to SGT 4. These bindings are forwarded by SXP to an SGACL enforcement device.

```
Device(config)# cts role-based sgt-map host 10.1.2.1 sgt 3
Device(config)# cts role-based sgt-map host 10.1.2.2 sgt 4
```

Related Commands

| Command | Description |
|------------------------------------|---|
| show cts role-based sgt-map | Displays role-based access control information. |

cts sxp connection peer

To enter the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) peer IP address, to specify if a password is used for the peer connection, to specify the global hold-time period for a listener or speaker device, and to specify if the connection is bidirectional, use the **cts sxp connection peer** command in global configuration mode. To remove these configurations for a peer connection, use the **no** form of this command.

```
cts sxp connection peer ipv4-address {source | password} {default | none} mode {local | peer}
[{{[[{listener | speaker}]] [{hold-time minimum-time maximum-time | vrf vrf-name}]] | both [vrf
vrf-name]}]
```

```
cts sxp connection peer ipv4-address {source | password} {default | none} mode {local | peer}
[{{[[{listener | speaker}]] [{hold-time minimum-time maximum-time | vrf vrf-name}]] | both [vrf
vrf-name]}]
```

Syntax Description

| | |
|---|---|
| <i>ipv4-address</i> | SXP peer IPv4 address. |
| source | Specifies the source IPv4 address. |
| password | Specifies that an SXP password is used for the peer connection. |
| default | Specifies that the default SXP password is used. |
| none | Specifies no password is used. |
| mode | Specifies either the local or peer SXP connection mode. |
| local | Specifies that the SXP connection mode refers to the local device. |
| peer | Specifies that the SXP connection mode refers to the peer device. |
| listener | (Optional) Specifies that the device is the listener in the connection. |
| speaker | (Optional) Specifies that the device is the speaker in the connection. |
| hold-time <i>minimum-time</i> <i>maximum-time</i> | (Optional) Specifies the hold-time period, in seconds, for the device. The range for minimum and maximum time is from 0 to 65535. A <i>maximum-time</i> value is required only when you use the following keywords: peer speaker and local listener . In other instances, only a <i>minimum-time</i> value is required. Note If both minimum and maximum times are required, the <i>maximum-time</i> value must be greater than or equal to the <i>minimum-time</i> value. |
| vrf <i>vrf-name</i> | (Optional) Specifies the virtual routing and forwarding (VRF) instance name to the peer. |
| both | (Optional) Specifies that the device is both the speaker and the listener in the bidirectional SXP connection. |

Command Default The CTS-SXP peer IP address is not configured and no CTS-SXP peer password is used for the peer connection. The default setting for a CTS-SXP connection password is **none**.

Command Modes Global configuration (config)

| Release | Modification |
|--------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines When a CTS-SXP connection to a peer is configured with the **cts sxp connection peer** command, only the connection mode can be changed. The **vrf** keyword is optional. If a VRF name is not provided or a VRF name is provided with the **default** keyword, then the connection is set up in the default routing or forwarding domain.

A **hold-time maximum-period** value is required only when you use the following keywords: **peer speaker** and **local listener**. In other instances, only a **hold-time minimum-period** value is required.



Note The *maximum-period* value must be greater than or equal to the *minimum-period* value.

Use the **both** keyword to configure a bidirectional SXP connection. With the support for bidirectional SXP configuration, a peer can act as both a speaker and a listener and propagate SXP bindings in both directions using a single connection.

Examples

The following example shows how to enable CTS-SXP and configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener:

```
Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the CTS-SXP peer connection on Device_B, a listener, for connection to Device_A, a speaker:

```
Device_B> enable
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

You can also configure both peer and source IP addresses for an SXP connection. The source IP address specified in the **cts sxp connection** command overwrites the default value.

```
Device_A(config)# cts sxp connection peer 51.51.51.1 source 51.51.51.2 password none mode local speaker
```

```
Device_B(config)# cts sxp connection peer 51.51.51.2 source 51.51.51.1 password none mode
local listener
```

The following example shows how to enable bidirectional CTS-SXP and configure the SXP peer connection on Device_A to connect to Device_B:

```
Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local both
```

Related Commands

| Command | Description |
|-----------------------------------|--|
| cts sxp default password | Configures the Cisco TrustSec SXP default password. |
| cts sxp default source-ip | Configures the Cisco TrustSec SXP source IPv4 address. |
| cts sxp enable | Enables Cisco TrustSec SXP on a device. |
| cts sxp log | Enables logging for IP-to-SGT binding changes. |
| cts sxp reconciliation | Changes the Cisco TrustSec SXP reconciliation period. |
| cts sxp retry | Changes the Cisco TrustSec SXP retry period timer. |
| cts sxp speaker hold-time | Configures the global hold-time period of a speaker device in a Cisco TrustSec SGT SXPv4 network. |
| cts sxp listener hold-time | Configures the global hold-time period of a listener device in a Cisco TrustSec SGT SXPv4 network. |
| show cts sxp | Displays the status of all Cisco TrustSec SXP configurations. |

cts sxp default password

To specify the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) default password, use the **cts sxp default password** command in global configuration mode. To remove the CTS-SXP default password, use the **no** form of this command.

```
cts sxp default password {0 unencrypted-pwd | 6 encrypted-key | 7 encrypted-keycleartext-pwd}
no cts sxp default password {0 unencrypted-pwd | 6 encrypted-key | 7 encrypted-keycleartext-pwd}
```

Syntax Description

| | |
|---------------------------------|--|
| 0 <i>unencrypted-pwd</i> | Specifies that an unencrypted CTS-SXP default password follows. The maximum password length is 32 characters. |
| 6 <i>encrypted-key</i> | Specifies that a 6 encryption type password is used as the CTS-SXP default password. The maximum password length is 32 characters. |
| 7 <i>encrypted-key</i> | Specifies that a 7 encryption type password is used as the CTS-SXP default password. The maximum password length is 32 characters. |
| <i>cleartext-pwd</i> | Specifies a cleartext CTS-SXP default password. The maximum password length is 32 characters. |

Command Default

Type **0** (cleartext)

Command Modes

Global configuration (config)

Command History

| Release | Modification |
|--------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines

The **cts sxp default password** command sets the CTS-SXP default password to be optionally used for all CTS-SXP connections configured on the device. The CTS-SXP password can be cleartext, or encrypted with the **0**, **7**, **6** encryption type keywords. If the encryption type is 0, then an unencrypted cleartext password follows.

Examples

The following example shows how to enable CTS-SXP and configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener:

```
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the CTS-SXP peer connection on Device_B, a listener, for connection to Device_A, a speaker:

```
Device_B# configure terminal
```

```

Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener

```

Related Commands

| Command | Description |
|----------------------------------|---|
| cts sxp connection peer | Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection. |
| cts sxp default source-ip | Configures the CTS-SXP source IPv4 address. |
| cts sxp enable | Enables CTS-SXP on a device. |
| cts sxp log | Enables logging for IP-to-SGT binding changes. |
| cts sxp reconciliation | Changes the CTS-SXP reconciliation period. |
| cts sxp retry | Changes the CTS-SXP retry period timer. |
| show cts sxp | Displays the status of all SXP configurations. |

cts sxp default source-ip

To configure the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) source IPv4 address, use the **cts sxp default source-ip** command in global configuration mode. To remove the CTS-SXP default source IP address, use the **no** form of this command.

```
cts sxp default source-ip ipv4-address
no cts sxp default source-ip ipv4-address
```

| | |
|---------------------------|--|
| Syntax Description | <i>ip-address</i> Default source CTS-SXP IPv4 address. |
|---------------------------|--|

Command Default The CTS-SXP source IP address is not configured.

Command Modes Global configuration (config)

| Command History | Release | Modification |
|------------------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines The **cts sxp default source-ip** command sets the default source IP address that CTS-SXP uses for all new TCP connections where a source IP address is not specified. Preexisting TCP connections are not affected when this command is entered. CTS-SXP connections are governed by three timers:

- Retry timer
- Delete Hold Down timer
- Reconciliation timer

Examples

The following example shows how to enable CTS-SXP and configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener:

```
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the CTS-SXP peer connection on Device_B, a listener, for connection to Device_A, a speaker:

```
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```


Related Commands

| Command | Description |
|---------------------------------|---|
| cts sxp connectionpeer | Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection. |
| cts sxp default password | Configures the CTS-SXP default password. |
| cts sxp enable | Enables CTS-SXP on a device. |
| cts sxp log | Enables logging for IP-to-SGT binding changes. |
| cts sxp reconciliation | Changes the CTS-SXP reconciliation period. |
| cts sxp retry | Changes the CTS-SXP retry period timer. |
| show cts sxp | Displays the status of all SXP configurations. |

cts sxp filter-enable

To enable filtering after creating filter lists and filter groups, use the **cts sxp filter-enable** command in global configuration mode. To disable filtering, use the **no** form of the command.

cts sxp filter-enable
no cts sxp filter-enable

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration (config)

Command History

| Release | Modification |
|--------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines

This command can be used at any time to enable or disable filtering. Configured filter lists and filter groups can be used to implement filtering only after filtering is enabled. The filter action will only filter bindings that are exchanged after filtering is enabled; there won't be any effect on the bindings that were exchanged before filtering was enabled.

Examples

```
Device(config)# cts sxp filter-enable
```

Related Commands

| Command | Description |
|------------------------------------|---|
| cts sxp filter-list | Creates a SXP filter list to filter IP-SGT bindings based on IP prefixes, SGT or a combination of both. |
| cts sxp filter-group | Creates a filter group for grouping a set of peers and applying a filter list to them. |
| show cts sxp filter-group | Displays information about the configured filter groups.. |
| show cts sxp filter-list | Displays information about the configured filter lists. |
| debug cts sxp filter events | Logs events related to the creation, deletion and update of filter-lists and filter-groups |

cts sxp filter-group

To create a filter group for grouping a set of peers and applying a filter list to them, use the **cts sxp filter-group** command in global configuration mode. To delete a filter group, use the **no** form of this command.

```
cts sxp filter-group {listener | speaker} {filter-group-name | global filter-list-name}
no cts sxp filter-group {listener | speaker} {filter-group-name | global filter-list-name}
```

| Syntax Description | | |
|--------------------|--------------------------|---|
| | listener | Creates a filter group for a set of listeners. |
| | speaker | Creates a filter group for a set of speakers. |
| | global | Groups all speakers or listeners on the device. |
| | <i>filter-group-name</i> | Name of the filter group. |
| | <i>filter-list-name</i> | Name of the filter list. |

Command Modes

Global configuration (config)

Command History

| Release | Modification |
|--------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines

Issuing this command, places the device in the filter group configuration mode. From this mode, you can specify the devices to be grouped and apply a filter list to the filter group.

The command format to add devices or peers to the group is as follows:

```
peer ipv4 peer-IP
```

In a single command, you can add one peer. To add more peers, repeat the command as many times as required.

The command format to apply a filter list to the group is as follows:

```
filter filter-list-name
```

You cannot specify a peer list for the global listener and global speaker filter-group options because in this case the filter is applied to all SXP connections.

When both the global filter group and peer-based filter groups are applied, the global filter takes priority. If only a global listener or global speaker filter group is configured, then the global filtering takes precedence only in that specific direction. For the other direction, the peer-based filter group is implemented.

Examples

The following example shows how to create a listener group called **group_1**, and assign peers and a filter list to this group:

```
Device# configure terminal
Device(config)# cts sxp filter-group listener group_1
Device(config-filter-group)# filter filter_1
```

```
Device(config-filter-group)# peer ipv4 10.0.0.1
Device(config-filter-group)# peer ipv4 10.10.10.1
```

The following example shows how to create a global listener group called **group_2**:

```
Device# configure terminal
Device(config)# cts sxp filter-group listener global group_2
```

Related Commands

| Command | Description |
|------------------------------------|---|
| cts sxp filter-list | Creates a SXP filter list to filter IP-SGT bindings based on IP prefixes, SGT or a combination of both. |
| cts sxp filter-enable | Enables filtering. |
| show cts sxp filter-group | Displays information about the configured filter groups. |
| show cts sxp filter-list | Displays information about the configured filter lists. |
| debug cts sxp filter events | Logs events related to the creation, deletion and update of filter-lists and filter-groups |

cts sxp filter-list

To create a SXP filter list to hold a set of filter rules for filtering IP-SGT bindings, use the **cts sxp filter-list** command in global configuration mode. To delete a filter list, use the **no** form of the command.

```
cts sxp filter-list filter-list-name
no cts sxp filter-list filter-list-name
```

Syntax Description

| | |
|-------------------------|--------------------------|
| <i>filter-list-name</i> | Name of the filter-list. |
|-------------------------|--------------------------|

Command Modes

Global configuration (config)

Command History

| Release | Modification |
|--------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines

Issuing this command, places the device in the filter list configuration mode. From this mode, you can specify rules for the filter lists.

A filter rule can be based on SGT or IP Prefixes or a combination of both SGT and IP Prefixes.

The command format to add rules to the group is as follows:

```
sequence-number action(permit/deny) filter-type(ipv4/ipv6/sgt) value/values
```

For example, to permit SGT-IP bindings whose SGT value is 20, the rule is as follows:

```
30 permit sgt 20
```

Note that the sequence number is optional. If you do not specify a sequence number, it is generated by the system. Sequence numbers are automatically incremented by a value of 10 from the last used/configured sequence number. A new rule can be inserted by specifying a sequence number in between two existing rules.

The range of valid SGT values is between 2 and 65519. To provide multiple SGT values in a rule, separate the values using a space. A maximum of 8 SGT values are allowed in a rule.

In a SGT and IP prefix combination rule, if there is a match for the binding in both the parts of the rule, then the action specified in the second part of the rule takes precedence. For example, in the following rule, if the SGT value of the IP prefix 10.0.0.1 is 20, the corresponding binding will be denied even if the first part of the rule permits the binding.

```
Device(config-filter-list)# 10 permit sgt 30 20 deny 10.0.0.1/24
```

Similarly, in the rule below the binding with the sgt value 20 will be permitted even if the sgt of the IP prefix 10.0.0.1 is 20, and the first action does not permit the binding.

```
Device(config-filter-list)# 10 deny 10.0.0.1/24 permit sgt 30 20
```

Examples

The following example shows how to create a filter list and add some rules to the list:

```

Device# configure terminal
Device(config)# cts sxp filter-list filter_1
Device (config-filter-list)# 10 deny ipv4 10.0.0.1/24 permit sgt 100
Device(config-filter-list)# 20 permit sgt 60 61 62 63

```

Related Commands

| Command | Description |
|------------------------------------|---|
| cts sxp filter-enable | Enable SXP IP-prefix and SGT-based filtering. |
| cts sxp filter-group | Creates a filter group for grouping a set of peers and applying a filter list to them. |
| show cts sxp filter-group | Displays information about the configured filter groups. |
| show cts sxp filter-list | Displays information about the configured filter lists. |
| debug cts sxp filter events | Logs events related to the creation, deletion and update of filter-lists and filter-groups. |

cts sxp log binding-changes

To enable logging for IP-to-Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) binding changes, use the **cts sxp log binding-changes** command in global configuration mode. To disable logging, use the **no** form of this command.

```
cts sxp log binding-changes
no cts sxp log binding-changes
```

Command Default Logging is disabled.

Command Modes Global configuration (config)

| Command History | Release | Modification |
|-----------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines The **cts sxp log binding-changes** command enables logging for IP-to-SGT binding changes. SXP syslogs (sev 5 syslogs) are generated whenever IP address-to-SGT binding occurs (add, delete, change). These changes are learned and propagated on the SXP connection.

| Related Commands | Command | Description |
|------------------|----------------------------------|--|
| | cts sxp connectionpeer | Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection |
| | cts sxp default password | Configures the CTS-SXP default password. |
| | cts sxp default source-ip | Configures the CTS-SXP source IPv4 address. |
| | cts sxp enable | Enables CTS-SXP on a device. |
| | cts sxp reconciliation | Changes the CTS-SXP reconciliation period. |
| | cts sxp retry | Changes the CTS-SXP retry period timer. |
| | show cts sxp | Displays status of all SXP configurations. |

cts sxp reconciliation period

To change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) reconciliation period, use the **cts sxp reconciliation period** command in global configuration mode. To return the CTS-SXP reconciliation period to its default value, use the **no** form of this command.

cts sxp reconciliation period *seconds*
no cts sxp reconciliation period *seconds*

| | |
|---------------------------|---|
| Syntax Description | <i>seconds</i> CTS-SXP reconciliation timer in seconds. The range is from 0 to 64000. The default is 120. |
|---------------------------|---|

Command Default 120 seconds (2 minutes)

Command Modes Global configuration (config)

| Command History | Release | Modification |
|------------------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines After a peer terminates a CTS-SXP connection, an internal delete hold-down timer starts. If the peer reconnects before the delete hold-down timer expires, then the CTS-SXP reconciliation timer starts. While the CTS-SXP reconciliation period timer is active, the CTS-SXP software retains the SGT mapping entries learned from the previous connection and removes invalid entries. Setting the SXP reconciliation period to 0 seconds disables the timer and causes all entries from the previous connection to be removed.

| Related Commands | Command | Description |
|-------------------------|----------------------------------|---|
| | cts sxp connection peer | Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection. |
| | cts sxp default password | Configures the CTS-SXP default password. |
| | cts sxp default source-ip | Configures the CTS-SXP source IPv4 address. |
| | cts sxp enable | Enables CTS-SXP on a device. |
| | cts sxp log | Turns on logging for IP to SGT binding changes. |
| | cts sxp retry | Changes the CTS-SXP retry period timer. |
| | show cts sxp | Displays status of all CTS-SXP configurations. |

cts sxp retry period

To change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) retry period timer, use the **cts sxp retry period** command in global configuration mode. To return the CTS-SXP retry period timer to its default value, use the **no** form of this command.

cts sxpretry period *seconds*
no cts sxpretry period *seconds*

| | |
|---------------------------|--|
| Syntax Description | <i>seconds</i> CTS-SXP retry timer in seconds. The range is from 0 to 64000. The default is 120. |
|---------------------------|--|

Command Default 120 seconds (2 minutes)

Command Modes Global configuration (config)

| Command History | Release | Modification |
|------------------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines The retry timer is triggered if there is at least one CTS-SXP connection that is not up. A new CTS-SXP connection is attempted when this timer expires. A zero value results in no retry being attempted.

| Related Commands | Command | Description |
|-------------------------|----------------------------------|---|
| | cts sxp connectionpeer | Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection. |
| | cts sxp default password | Configures the CTS-SXP default password. |
| | cts sxp default source-ip | Configures the CTS-SXP source IPv4 address. |
| | cts sxp enable | Enables CTS-SXP on a device. |
| | cts sxp log | Enables logging for IP-to-SGT binding changes. |
| | cts sxp reconciliation | Changes the CTS-SXP reconciliation period. |
| | show cts sxp | Displays the status of all CTS-SXP configurations. |

propagate sgt (cts manual)

To enable Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces, use the **propagate sgt** command in interface configuration mode. To disable SGT propagation, use the **no** form of this command.

propagate sgt

Syntax Description

This command has no arguments or keywords.

Command Default

SGT processing propagation is enabled.

Command Modes

CTS manual interface configuration mode (config-if-cts-manual)

Command History

| Release | Modification |
|--------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines

SGT processing propagation allows a CTS-capable interface to accept and transmit a CTS Meta Data (CMD) based L2 SGT tag. The **no propagate sgt** command can be used to disable SGT propagation on an interface in situations where a peer device is not capable of receiving an SGT, and as a result, the SGT tag cannot be put in the L2 header.

Examples

The following example shows how to disable SGT propagation on a manually-configured TrustSec-capable interface:

```
Device# configure terminal
Device(config)# interface gigabitethernet 0
Device(config-if)# cts manual
Device(config-if-cts-manual)# no propagate sgt
```

The following example shows that SGT propagation is disabled on Gigabit Ethernet interface 0:

```
Device#show cts interface brief
Global Dot1x feature is Disabled
Interface GigabitEthernet0:
  CTS is enabled, mode:      MANUAL
  IFC state:                OPEN
  Authentication Status:    NOT APPLICABLE
  Peer identity:            "unknown"
  Peer's advertised capabilities: ""
  Authorization Status:     NOT APPLICABLE
  SAP Status:               NOT APPLICABLE
  Propagate SGT:           Disabled
  Cache Info:
    Cache applied to link : NONE
```

Related Commands

| Command | Description |
|-------------------|-------------------------------|
| cts manual | Enables an interface for CTS. |

| Command | Description |
|---------------------------|--|
| show cts interface | Displays Cisco TrustSec states and statistics per interface. |

sap mode-list (cts manual)

To select the Security Association Protocol (SAP) authentication and encryption modes (prioritized from highest to lowest) used to negotiate link encryption between two interfaces, use the **sap mode-list** command in CTS dot1x interface configuration mode. To remove a mode-list and revert to the default, use the **no** form of this command.

Use the **sap mode-list** command to manually specify the Pairwise Master Key (PMK) and the Security Association Protocol (SAP) authentication and encryption modes to negotiate MACsec link encryption between two interfaces. Use the **no** form of the command to disable the configuration.

sap pmk mode-list {gcm-encrypt | gmac | no-encap | null} [gcm-encrypt | gmac | no-encap | null]

no sap pmk mode-list {gcm-encrypt | gmac | no-encap | null} [gcm-encrypt | gmac | no-encap | null]

Syntax Description

| | |
|-----------------------------|---|
| pmk <i>hex_value</i> | Specifies the Hex-data PMK (without leading 0x; enter even number of hex characters, or else the last character is prefixed with 0.). |
| mode-list | Specifies the list of advertised modes (prioritized from highest to lowest). |
| gcm-encrypt | Specifies GMAC authentication, GCM encryption. |
| gmac | Specifies GMAC authentication only, no encryption. |
| no-encap | Specifies no encapsulation. |
| null | Specifies encapsulation present, no authentication, no encryption. |

Command Default

The default encryption is **sap pmk mode-list gcm-encrypt null**. When the peer interface does not support 802.1AE MACsec or 802.REV layer-2 link encryption, the default encryption is **null**.

Command Modes

CTS manual interface configuration (config-if-cts-manual)

Command History

| Release | Modification |
|--------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines

Use the **sap pmk mode-list** command to specify the authentication and encryption method.

The Security Association Protocol (SAP) is an encryption key derivation and exchange protocol based on a draft version of the 802.11i IEEE protocol. SAP is used to establish and maintain the 802.1AE link-to-link encryption (MACsec) between interfaces that support MACsec.

SAP and the Pairwise Master Key (PMK) can be manually configured between two interfaces with the **sap pmk mode-list** command. When using 802.1X authentication, both sides (supplicant and authenticator) receive the PMK and the MAC address of the peer's port from the Cisco Secure Access Control Server.

If a device is running CTS-aware software but the hardware is not CTS-capable, disallow encapsulation with the **sap mode-list no-encap** command.

Examples

The following example shows how to configure SAP on a Gigabit Ethernet interface:

```
Device# configure terminal
Device(config)# interface gigabitethernet 2/1
DeviceD(config-if)# cts manual
Device(config-if-cts-manual)# sap pmk FFEF mode-list gcm-encrypt
```

Related Commands

| Command | Description |
|-----------------------------------|--|
| cts manual | Enables an interface for CTS. |
| propagate sgt (cts manual) | Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces. |
| show cts interface | Displays Cisco TrustSec interface configuration statistics. |

show cts credentials

To display the Cisco TrustSec (CTS) device ID, use the **show cts credentials** command in EXEC or privileged EXEC mode.

show cts credentials

Syntax Description

This command has no commands or keywords.

Command Modes

Privileged EXEC (#) User EXEC (>)

Command History

| Release | Modification |
|--------------------------|------------------------------|
| Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Examples

The following example displays output:

```
Device# show cts credentials
```

```
CTS password is defined in keystore, device-id = r4
```

Related Commands

| Command | Description |
|------------------------|---|
| cts credentials | Specifies the TrustSec ID and password. |

show cts interface

To display Cisco TrustSec (CTS) configuration statistics for an interface(s), use the **show cts interface** command in EXEC or privileged EXEC mode.

show cts interface [{**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**}]

| Syntax Description | |
|--------------------|---|
| <i>port</i> | (Optional) Gigabit Ethernet interface number. A verbose status output for this interface is returned. |
| <i>number</i> | (Optional) VLAN interface number from 1 to 4095. |
| brief | (Optional) Displays abbreviated status for all CTS interfaces. |
| summary | (Optional) Displays a tabular summary of all CTS interfaces with 4 or 5 key status fields for each interface. |

Command Default None

Command Modes
 EXEC (>)
 Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines Use the **show cts interface** command without keywords to display verbose status for all CTS interfaces.

Examples The following example displays output without using a keyword (verbose status for all CTS interfaces):

```
Device# show cts interface

Global Dot1x feature is Disabled
Interface GigabitEthernet0/1/0:
  CTS is enabled, mode:    MANUAL
  IFC state:              OPEN
  Interface Active for 00:00:18.232
  Authentication Status:  NOT APPLICABLE
  Peer identity:          "unknown"
  Peer's advertised capabilities: ""
  Authorization Status:   NOT APPLICABLE
  SAP Status:             NOT APPLICABLE
  Configured pairwise ciphers:
    gcm-encrypt
    null

  Replay protection:      enabled
  Replay protection mode: STRICT

  Selected cipher:
```

```

Propagate SGT:          Enabled
Cache Info:
  Cache applied to link : NONE

Statistics:
  authc success:        0
  authc reject:         0
  authc failure:        0
  authc no response:    0
  authc logoff:         0
  sap success:          0
  sap fail:             0
  authz success:        0
  authz fail:           0
  port auth fail:       0
  Ingress:
    control frame bypassed: 0
    sap frame bypassed:    0
    esp packets:           0
    unknown sa:            0
    invalid sa:            0
    inverse binding failed: 0
    auth failed:           0
    replay error:          0
  Egress:
    control frame bypassed: 0
    esp packets:           0
    sgt filtered:          0
    sap frame bypassed:    0
    unknown sa dropped:    0
    unknown sa bypassed:   0

```

The following example displays output using the **brief** keyword:

```

Device# show cts interface brief

Global Dot1x feature is Disabled
Interface GigabitEthernet0/1/0:
  CTS is enabled, mode:    MANUAL
  IFC state:              OPEN
  Interface Active for 00:00:40.386
  Authentication Status:  NOT APPLICABLE
  Peer identity:          "unknown"
  Peer's advertised capabilities: ""
  Authorization Status:   NOT APPLICABLE
  SAP Status:             NOT APPLICABLE
  Propagate SGT:          Enabled
  Cache Info:
    Cache applied to link : NONE

```

Related Commands

| Command | Description |
|-----------------------|--|
| cts manual | Enables an interface for CTS. |
| cts sxp enable | Configures SXP on a network device. |
| propagate sgt | Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces. |

show cts role-based counters

To display Security Group access control list (ACL) enforcement statistics, use the **show cts role-based counters** command in user EXEC or privileged EXEC mode.

```
show cts role-based counters [{default [{ipv4 | ipv6}]}] [{from {sgt-number | unknown} [{ipv4 | ipv6} | to | {sgt-number | unknown} ] [{ipv4 | ipv6}]}] [{to {sgt-number | unknown} [{ipv4 | ipv6}]}]
[{ipv4 | ipv6}]
```

| Syntax Description | | |
|--------------------|--|---|
| default | | (Optional) Displays information about the default policy counters. |
| from | | (Optional) Displays information about the source security group. |
| ipv4 | | (Optional) Displays information about security groups on IPv4 networks. |
| ipv6 | | (Optional) Displays information about security groups on IPv6 networks. |
| to | | (Optional) Displays information about the destination security group. |
| <i>sgt-number</i> | | (Optional) Security Group Tag number. Valid values are from 0 to 65533. |
| unknown | | (Optional) Displays information about all source groups. |

| Command Modes | |
|---------------|---------------------|
| | User EXEC (>) |
| | Privileged EXEC (#) |

| Command History | Release | Modification |
|-----------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

| Usage Guidelines | |
|------------------|--|
| | Use the clear cts role-based counters command to reset all or a range of statistics. |
| | Specify the source SGT with the from keyword and the destination SGT with the to keyword. All statistics are displayed when both the from and to keywords are omitted. |
| | The default keyword displays the statistics of the default unicast policy. When neither ipv4 nor ipv6 keywords are specified, this command displays only IPv4 counters. |
| | In Cisco TrustSec monitor mode, permitted traffic counters are displayed under the SW-Permitt label and the denied traffic counters are displayed under SW-Monitor label. |

Example

The following is sample output from the **show cts role-based counters**

```
Device# show cts role-based counters
```

```
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt  HW-Permitt  SW-Monitor  HW-Monitor
12      24      0           0           0           0           0           0
12      77      0           0           5           0           0           0
```

The table below lists the significant fields shown in the display.

Table 1: show cts role-based counters Field Descriptions

| Field | Description |
|------------|-----------------------------|
| From | Source security group. |
| To | Destination security group. |
| SW-Permitt | Permitted traffic counters. |
| SW-Monitor | Denied traffic counters. |

Related Commands

| Command | Description |
|---------------------------------|--|
| clear role-basedcounters | Resets SGACL statistic counters. |
| cts role-based | Maps IP addresses, Layer 3 interfaces, and VRFs to SGTs. Enables Cisco TrustSec caching and SGACL enforcement. |

show cts role-based permissions

To display the role-based (security group) access control permission list, use the **show cts role-based permissions** command in privileged EXEC mode.

```
show cts role-based permissions [{default [{details | ipv4 [details] | ipv6 [details]]} | from {{sgt | unknown}}[{{ipv4 | ipv6 | to {{sgt | unknown}}[{{details | ipv4 [details] | ipv6 [details]}]}]}] | ipv4 | ipv6 | platform | to {sgt | unknown}[{{ipv4 | ipv6}}]}
```

| Syntax Description | default | (Optional) Displays information about the default permission list. |
|--------------------|-----------------|--|
| | details | (Optional) Displays attached access control list (ACL) details. |
| | ipv4 | (Optional) Displays information about the IPv4 protocol. |
| | ipv6 | (Optional) Displays information about the IPv6 protocol. |
| | from | (Optional) Displays information about the source group. |
| | <i>sgt</i> | (Optional) Security Group Tag. Valid values are from 2 to 65519. |
| | to | (Optional) Displays information about the destination group. |
| | unknown | (Optional) Displays information about unknown source and destination groups. |
| | platform | (Optional) Displays information about the platform. |

Command Modes Privileged EXE (#)

| Command History | Release | Modification |
|-----------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Usage Guidelines This command displays the content of the SGACL permission matrix. You can specify the source security group tag (SGT) by using the **from** keyword and the destination SGT by using the **to** keyword. When both these keywords are specified RBACLs of a single cell are displayed. An entire column is displayed when only the **to** keyword is used. An entire row is displayed when the **from** keyword is used. The entire permission matrix is displayed when both the **from** and **to** keywords are omitted.

The command output is sorted by destination SGT as a primary key and the source SGT as a secondary key. SGACLs for each cell is displayed in the same order they are defined in the configuration or acquired from Cisco Identity Services Engine (ISE).

The **details** keyword is provided when a single cell is selected by specifying both **from** and **to** keywords. When the **details** keyword is specified the access control entries of SGACLs of a single cell are displayed.

The following is sample output from the **show role-based permissions** command:

```
Device# show cts role-based permissions
```

show cts role-based permissions

```

IPv4 Role-based permissions default (monitored):
default_sgacl-02
Permit IP-00
IPv4 Role-based permissions from group 305:sgt to group 306:dgt (monitored):
test_reg_tcp_permit-02
RBACL Monitor All for Dynamic Policies : TRUE
RBACL Monitor All for Configured Policies : FALSE
IPv4 Role-based permissions from group 6:SGT_6 to group 6:SGT_6 (configured):
  mon_1
IPv4 Role-based permissions from group 10 to group 11 (configured):
  mon_2
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

```

Related Commands

| Command | Description |
|-----------------------------------|---|
| cts role-based permissions | Enables permissions from a source group to a destination group. |
| cts role-based monitor | Enables role-based access list monitoring. |

show cts server-list

To display the list of HTTP and RADIUS servers available to Cisco TrustSec seed and nonseed devices, use the **show cts server-list** command in user EXEC or privileged EXEC mode.

show cts server-list

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC (>)
Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------------------------|--|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |
| | Cisco IOS XE Amsterdam 17.1.1 | The output of this command was modified to display the HTTP server address and status information. |
| | Cisco IOS XE Amsterdam 17.2.1 | The output of this command was modified to display the IPv6 address of the HTTP servers. |

Usage Guidelines This command is useful for gathering Cisco TrustSec RADIUS server address and status information.

In Cisco IOS XE Gibraltar 17.1.1 and later releases, the output of this command displays HTTP server address and their status information.

In Cisco IOS XE Gibraltar 17.2.1 and later releases, the output of this command displays the IPv6 address along with the IPv4 address of HTTP servers.

Examples

Cisco IOS XE Amsterdam 17.2.1 and later releases

The following sample output from the **show cts server-list** command displays IPv4 and IPv6 address of HTTP servers and their status information:

```
Device> show cts server-list

HTTP Server-list:
  Server Name   : cts_private_server_0
  Server State  : ALIVE
  IPv4 Address  : 10.64.69.151
  IPv6 Address  : 2001:DB8:8086:6502::
  IPv6 Address  : 2001:db8::2
  IPv6 Address  : 2001:db8::402:99
  IPv6 Address  : 2001:DB8::802:16
  Domain-name   : ise-267.cisco.com
  Trustpoint    : cts_trustpoint_0

  Server Name   : cts_private_server_1
  Server State  : ALIVE
  IPv4 Address  : 10.10.10.3
  IPv4 Address  : 10.10.10.2
  IPv6 Address  : 2001:db8::20
  IPv6 Address  : 2001:db8::21
```

show cts server-list

```
Domain-name      : www.ise.cisco.com
Trustpoint       : cts_trustpoint_1
```

Cisco IOS XE Amsterdam 17.1.1

The following sample output from the **show cts server-list** command displays HTTP servers and their status information:

```
Device> show cts server-list

HTTP Server-list:
Server Name: Http_Server_1
Server Status: DEAD
  IPv4 Address: 10.78.105.148
  IPv6 Address: Not Supported
  Domain-name: http_server_1.ise.com
  Port: 9063

Server Name: Http_Server_2
Server Status: ALIVE
  IPv4 Address: 10.78.105.149
  IPv6 Address: Not Supported
  Domain-name: http_server_2.ise.com
  Status = ALIVE
```

Prior to Cisco IOS XE Amsterdam 17.1.1

The following example displays the Cisco TrustSec RADIUS server list:

```
Device> show cts server-list

CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)
Preferred list, 1 server(s):
 *Server: 10.0.1.6, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
   Status = ALIVE
   auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: ACSServerList1-0001, 1 server(s):
 *Server: 101.0.2.61, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
   Status = ALIVE
   auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

Related Commands

| Command | Description |
|--|---|
| address ipv4 (config-radius-server) | Configures the RADIUS server accounting and authentication parameters for PAC provisioning. |
| pac key | Specifies the PAC encryption key. |

show cts sxp

To display Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) connection or source IP-to-SGT mapping information, use the **show cts sxp** command in user EXEC or privileged EXEC mode.

```
show cts sxp {connections [{brief | vrf instance-name}] | filter-group [{detailed | global | listener | speaker }]} | filter-list filter-list-name | sgt-map [{brief | vrf instance-name}]
```

| Syntax Description | connections | Displays Cisco TrustSec SXP connections information. |
|--------------------|---|---|
| | brief | (Optional) Displays an abbreviation of the SXP information. |
| | vrf instance-name | (Optional) Displays the SXP information for the specified Virtual Routing and Forwarding (VRF) instance name. |
| | filter-group {detailed global listener speaker } | (Optional) Displays filter group information. |
| | filter-list filter-list-name | (Optional) Displays filter list information. |
| | sgt-map | (Optional) Displays the IP-to-SGT mappings received through SXP. |

Command Default None

Command Modes
User EXEC (>)
Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|--------------------------|------------------------------|
| | Cisco IOS XE Fuji 16.9.1 | This command was introduced. |

Examples

The following example displays the SXP connections using the **brief** keyword:

```
Device# show cts sxp connection brief

SXP                : Enabled
Default Password   : Set
Default Source IP  : Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
-----
Peer_IP           Source_IP           Conn Status         Duration
-----
10.10.10.1         10.10.10.2          On                   0:00:02:14 (dd:hr:mm:sec)
10.10.2.1          10.10.2.2           On                   0:00:02:14 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

The following example displays the CTS-SXP connections:

```
Device# show cts sxp connections

SXP           : Enabled
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
-----
Peer IP       : 10.10.10.1
Source IP     : 10.10.10.2
Set up        : Peer
Conn status   : On
Connection mode : SXP Listener
Connection inst# : 1
TCP conn fd   : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
-----
Peer IP       : 10.10.2.1
Source IP     : 10.10.2.2
Set up        : Peer
Conn status   : On
Connection mode : SXP Listener
TCP conn fd   : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

The following example displays the CTS-SXP connections for a bi-directional connection when the device is both the speaker and listener:

```
Device# show cts sxp connections

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
-----
Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)
```

The following example displays output from a CTS-SXP listener with a torn down connection to the SXP speaker. Source IP-to-SGT mappings are held for 120 seconds, the default value of the delete hold down timer.

```
Device# show cts sxp connections
```



```

SXP                : Enabled
Default Password   : Set
Default Source IP  : Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
-----
Peer IP            : 10.10.10.1
Source IP          : 10.10.10.2
Set up             : Peer
Conn status        : Delete_Hold_Down
Connection mode    : SXP Listener
Connection inst#   : 1
TCP conn fd        : -1
TCP conn password: not set (using default SXP password)
Delete hold down timer is running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)
-----
Peer IP            : 10.10.2.1
Source IP          : 10.10.2.2
Set up             : Peer
Conn status        : On
Connection inst#   : 1
TCP conn fd        : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)
Total num of SXP Connections = 2

```

Related Commands

| Command | Description |
|----------------------------------|---|
| cts sxp connection peer | Enters the Cisco TrustSec SXP peer IP address and specifies if a password is used for the peer connection |
| cts sxp default password | Configures the Cisco TrustSec SXP default password. |
| cts sxp default source-ip | Configures the Cisco TrustSec SXP source IPv4 address. |
| cts sxp enable | Enables Cisco TrustSec SXP on a device. |
| cts sxp log | Enables logging for IP-to-SGT binding changes. |
| cts sxp reconciliation | Changes the Cisco TrustSec SXP reconciliation period. |
| cts sxp retry | Changes the Cisco TrustSec SXP retry period timer. |

show platform hardware fed switch active fwd-asic resource tcam utilization

To display CAM utilization information for ASIC, use the **show platform hardware fed switch active fwd-asic resource tcam utilization** command in privileged EXEC mode.

show platform hardware fed switch active fwd-asic resource tcam utilization [*asic-number*] [*slice-id*]

| | |
|---------------------------|---|
| Syntax Description | asic-number ASIC number. Valid values are from 0 to 7. |
| | slice-id Displays per slice usage. |

Command Modes Privileged EXEC (#)

| | | |
|------------------------|-----------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

Examples

The following is sample output from the **show platform hardware fed switch active fwd-asic resource tcam utilization** command:

```
Device# enable
Device# show platform hardware fed switch active fwd-asic resource tcam utilization

CAM Utilization for ASIC [0]
Table          Subtype   Dir    Max    Used    %Used    V4     V6
MPLS    Other
-----
Mac Address Table    EM        I     32768    25    0.08%     0     0
  0      25
Mac Address Table    TCAM      I     1024    22    2.15%     0     0
  0      22
L3 Multicast         EM        I     8192     0    0.00%     0     0
  0      0
L3 Multicast         TCAM      I      512     9    1.76%     3     6
  0      0
L2 Multicast         EM        I     8192     0    0.00%     0     0
  0      0
L2 Multicast         TCAM      I      512    11    2.15%     3     8
  0      0
IP Route Table      EM        I    24576    14    0.06%    13     0
  1      0
IP Route Table      TCAM      I     8192    30    0.37%    11    16
  2      1
QOS ACL             TCAM      IO    5120    85    1.66%    28    38
  0      19
                   TCAM      I      45    0.88%    15    20
  0      10
                   TCAM      O      40    0.78%    13    18
  0      9
```

```

Security ACL          TCAM      IO      5120    131    2.56%    26     60
  0      45
      0      40          TCAM      I        88     1.72%    12     36
      0      5          TCAM      O        43     0.84%    14     24
Netflow ACL          TCAM      I      256     6     2.34%    2       2
  0      2
PBR ACL              TCAM      I     1024    36    3.52%    30       6
  0      0
Netflow ACL          TCAM      O      768     6     0.78%    2       2
  0      2
Flow SPAN ACL        TCAM      IO     1024    13    1.27%    3       6
  0      4
      0      2          TCAM      I         5     0.49%    1       2
      0      2          TCAM      O         8     0.78%    2       4
Control Plane        TCAM      I      512    290   56.64%   138    106
  0      46
Tunnel Termination   TCAM      I      512     22    4.30%    9       13
  0      0
Lisp Inst Mapping     TCAM      I     2048     2    0.10%    0        0
  0      2
Security Association  TCAM      I      256     4    1.56%    2        2
  0      0
CTS Cell Matrix/VPN  EM        O     8192     0    0.00%    0        0
Label 0 0
CTS Cell Matrix/VPN  TCAM      O      512     1    0.20%    0        0
Label 0 1
Client Table          EM        I     4096     0    0.00%    0        0
  0      0
Client Table          TCAM      I      256     0    0.00%    0        0
  0      0
Input Group LE        TCAM      I     1024     0    0.00%    0        0
  0      0
Output Group LE       TCAM      O     1024     0    0.00%    0        0
  0      0
Macsec SPD            TCAM      I      256     2    0.78%    0        0
  0      2

```

Output fields are self-explanatory.

Related Commands

| Command | Description |
|--|-----------------------------|
| show platform hardware fed switch active fwd-asic resource tcam usage | Displays current CAM usage. |
| show platform hardware fed switch active fwd-asic resource tcam table | Displays current CAM table. |

show platform hardware fed switch active sgACL resource usage

To display SGACL resource information for ASIC, use the **show platform hardware fed switch active sgACL resource usage** command in privileged EXEC mode.

show platform hardware fed switch active sgACL resource usage

Syntax Description **usage** Displays SGACL resource usage.

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

Examples

The following is sample output from the **show platform hardware fed switch active sgACL resource usage** command:

```
Device# enable
Device# show platform hardware fed switch active sgACL resource usage

SGACL RESOURCE DETAILS ASIC :#0
=====
Hardware Resource           MAX      Used      Percent
                               Used      Used      Used
-----
CTS Cell Matrix Config    :           :           :
CTS Cell Matrix Entries   :  8192    0         0
CTS Cell Overflow Entries :   512    1         0

Policy Configuration      :           :           :
Policy Entries            :   256    3         1

DGT Config                :           :           :
DGT Entries               :  4096    0         0

Security ACL Configured   :           :           :
Security ACL Entries      :   5120   131       2

                               Total      Percent
                               Used      Used
-----
Output PRE SGACL          :         4      12
Output SGACL              :         0       0
Output SGACL DEFAULT      :         0       0

.
.
.
Device#
```

Output fields are self-explanatory.

show platform software classification switch active F0 class-group-manager class-group client acl all

To display ACL class group ID, which is used to view Ternary Content Addressable Memory(TCAM) entry, use the **show platform software classification switch active F0 class-group-manager class-group client acl all** command in privileged EXEC mode.

show platform software classification switch active F0 class-group-manager class-group client acl all

Syntax Description

| | |
|----------------------------|---|
| class-group-manager | Displays the class group manager. |
| class-group | Displays the class group. |
| all | Displays the ACL class group ID for all class groups. |

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|-----------------------------|------------------------------|
| Cisco IOS XE Everest 16.6.1 | This command was introduced. |

Example

The following is sample output from the **show platform software classification switch active F0 class-group-manager class-group client acl all** command:

```
Device#show platform software classification switch active F0 class-group-manager class-group
client acl all
```

```
QFP classification class client all group
```

```
class-group [ACL-GRP:273]
class-group [ACL-GRP:529]
class-group [ACL-GRP:801]
```

Output fields are self-explanatory.

Related Commands

| Command | Description |
|---|--|
| show platform software classification switch active F0 class-group-manager class-group client acl name <i>class-group name</i> | Displays ACL class-group info for the specified class group. |
| show platform software classification switch active F0 class-group-manager class-group client acl <i>class-group id</i> | Displays ACL class-group info for the specified class group. |

show platform software cts forwarding-manager switch active F0 port

To display CTS information for forwarding manager interfaces, use the **show platform software cts forwarding-manager switch active F0 port** command in privileged EXEC mode.

show platform software cts forwarding-manager switch active F0 port

| Syntax Description | F0 Embedded-Service-Processor slot 0. | | | | |
|-----------------------------|---|---------|--------------|-----------------------------|------------------------------|
| | port Displays the port CTS status. | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Everest 16.6.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Everest 16.6.1 | This command was introduced. | | | | |

Example

The following is sample output from the **show platform software cts forwarding-manager switch active F0 port** command:

```
Device#show platform software cts forwarding-manager switch active F0 port
```

```
Forwarding Manager Interfaces CTS Information
```

| Name | ID | CTS Enable | Trusted | Propagate | SGT value |
|-----------------------|-----|------------|---------|-----------|-----------|
| GigabitEthernet1/0/1 | 77 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/3 | 79 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/4 | 80 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/5 | 81 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/6 | 82 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/7 | 83 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/8 | 84 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/9 | 85 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/10 | 86 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/11 | 87 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/12 | 88 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/13 | 89 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/14 | 90 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/15 | 91 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/16 | 92 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/17 | 93 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/18 | 94 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/19 | 95 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/20 | 96 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/21 | 97 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/22 | 98 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/23 | 99 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/24 | 100 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/25 | 101 | 0 | 0 | 0 | 0 |

| | | | | | |
|-----------------------|-----|---|---|---|---|
| GigabitEthernet1/0/26 | 102 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/27 | 103 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/28 | 104 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/29 | 105 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/30 | 106 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/31 | 107 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/32 | 108 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/33 | 109 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/34 | 110 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/35 | 111 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/36 | 112 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/37 | 113 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/38 | 114 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/39 | 115 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/40 | 116 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/41 | 117 | 0 | 0 | 0 | 0 |

Forwarding Manager Interfaces CTS Information

| Name | ID | CTS Enable | Trusted | Propagate | SGT value |
|---------------------------|-----|------------|---------|-----------|-----------|
| GigabitEthernet1/0/42 | 118 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/43 | 119 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/44 | 120 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/45 | 121 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/46 | 122 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/47 | 123 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/1/1 | 125 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/1/2 | 126 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/1/3 | 127 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/1/4 | 128 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet1/1/1 | 129 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet1/1/2 | 130 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet1/1/3 | 131 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet1/1/4 | 132 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet1/1/5 | 133 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet1/1/6 | 134 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet1/1/7 | 135 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet1/1/8 | 136 | 0 | 0 | 0 | 0 |
| FortyGigabitEthernet1/1/1 | 137 | 0 | 0 | 0 | 0 |
| FortyGigabitEthernet1/1/2 | 138 | 0 | 0 | 0 | 0 |
| TwentyFiveGigE1/1/1 | 139 | 0 | 0 | 0 | 0 |
| TwentyFiveGigE1/1/2 | 140 | 0 | 0 | 0 | 0 |
| AppGigabitEthernet1/0/1 | 141 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/1 | 142 | 1 | 0 | 0 | 0 |
| GigabitEthernet2/0/2 | 143 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/3 | 144 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/4 | 145 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/5 | 146 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/6 | 147 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/7 | 148 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/8 | 149 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/9 | 150 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/10 | 151 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/11 | 152 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/12 | 153 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/13 | 154 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/14 | 155 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/15 | 156 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/16 | 157 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/17 | 158 | 0 | 0 | 0 | 0 |

show platform software cts forwarding-manager switch active F0 port

Forwarding Manager Interfaces CTS Information

| Name | ID | CTS Enable | Trusted | Propagate | SGT value |
|-------------------------|-----|------------|---------|-----------|-----------|
| GigabitEthernet2/0/18 | 159 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/19 | 160 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/20 | 161 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/21 | 162 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/22 | 163 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/23 | 164 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/24 | 165 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/25 | 166 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/26 | 167 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/27 | 168 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/28 | 169 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/29 | 170 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/30 | 171 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/31 | 172 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/32 | 173 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/33 | 174 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/34 | 175 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/35 | 176 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/36 | 177 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/37 | 178 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/38 | 179 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/39 | 180 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/40 | 181 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/41 | 182 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/42 | 183 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/43 | 184 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/44 | 185 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/45 | 186 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/46 | 187 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/0/47 | 188 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/1/1 | 190 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/1/2 | 191 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/1/3 | 192 | 0 | 0 | 0 | 0 |
| GigabitEthernet2/1/4 | 193 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet2/1/1 | 194 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet2/1/2 | 195 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet2/1/3 | 196 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet2/1/4 | 197 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet2/1/5 | 198 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet2/1/6 | 199 | 0 | 0 | 0 | 0 |

Forwarding Manager Interfaces CTS Information

| Name | ID | CTS Enable | Trusted | Propagate | SGT value |
|---------------------------|-----|------------|---------|-----------|-----------|
| TenGigabitEthernet2/1/7 | 200 | 0 | 0 | 0 | 0 |
| TenGigabitEthernet2/1/8 | 201 | 0 | 0 | 0 | 0 |
| FortyGigabitEthernet2/1/1 | 202 | 0 | 0 | 0 | 0 |
| FortyGigabitEthernet2/1/2 | 203 | 0 | 0 | 0 | 0 |
| TwentyFiveGigE2/1/1 | 204 | 0 | 0 | 0 | 0 |
| TwentyFiveGigE2/1/2 | 205 | 0 | 0 | 0 | 0 |
| AppGigabitEthernet2/0/1 | 206 | 0 | 0 | 0 | 0 |
| GigabitEthernet1/0/2 | 213 | 0 | 0 | 0 | 0 |

The following table explains the significant fields shown in the output:

| Field | Description |
|-------|-------------|
|-------|-------------|

| | |
|---------------|--|
| Name | The name of the interface. |
| ID | The interface ID. |
| CTS Enable | The status of CTS. |
| Trusted | The trusted status of the interface. |
| Propagate | The propagate status of the interface. |
| SGT value | The value of SGT |

show platform software cts forwarding-manager switch active F0

To display SGT binding table, use the **show platform software cts forwarding-manager switch active F0** command in privileged EXEC mode.

show platform software cts forwarding-manager switch active F0

| Syntax Description | F0 Embedded-Service-Processor slot 0. | | | | |
|-----------------------------|---|---------|--------------|-----------------------------|------------------------------|
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Everest 16.6.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Everest 16.6.1 | This command was introduced. | | | | |

Example

The following is sample output from the **show platform software cts forwarding-manager switch active F0** command:

```
Device#show platform software cts forwarding-manager switch active F0

SGT Binding Table

Number of bindings: 1

2.2.2.2/32
SGT Src: 2
SGT Dst: 2
```

SGT Binding Table

Output fields are self-explanatory.

| Related Commands | Command | Description |
|------------------|---|---------------------------------|
| | show platform software cts forwarding-manager switch active F0 port | Displays the port CTS status. |
| | show platform software cts forwarding-manager switch active F0 permissions | Displays the SGACL permissions. |

show platform software cts forwarding-manager switch active F0 permissions

To display SGACL permissions, use the **show platform software cts forwarding-manager switch active F0 permissions** command in privileged EXEC mode.

show platform software cts forwarding-manager switch active F0 permissions

| Syntax Description | F0 Embedded-Service-Processor slot 0. | | | | |
|-----------------------------|---|---------|--------------|-----------------------------|------------------------------|
| | permissions Displays SGACL permissions. | | | | |
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Everest 16.6.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Everest 16.6.1 | This command was introduced. | | | | |

Example

The following is sample output from the **show platform software cts forwarding-manager switch active F0 permissions** command:

```
Device#show platform software cts forwarding-manager switch active F0 permissions
```

```
Forwarding Manager CTS permissions Information
```

```
 sgt      dgt      ACL Group Name
```

```
  4        2      V4SGACL7100
```

```
65535     65535   V4SGACL8100
```

```
65535     65535   V6SGACL9100
```

The following table explains the significant fields shown in the output:

| Field | Description |
|----------------|----------------------------|
| sgt | The source group tag. |
| dgt | The destination group tag. |
| ACL Group Name | The name of the ACL group. |

show platform software fed switch active acl counters hardware | inc SGACL

To display counters from the Forwarding Engine Driver, use the **show platform software fed switch active acl counters hardware | inc SGACL** command in privileged EXEC mode.

show platform software fed switch active acl counters hardware | inc SGACL

| Syntax Description | |
|--------------------|---|
| counters | Displays counter information. |
| hardware | Displays hardware counters. |
| include | Includes lines that match the specified string. |

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

Example

The following is sample output from the **show platform software fed switch active acl counters hardware | inc SGACL** command:

```
Device# show platform software fed switch active acl counters hardware | inc SGACL
Egress IPv4 SGACL Drop (0x3f000061): 0 frames
Egress IPv6 SGACL Drop (0x13000062): 0 frames
Egress IPv4 SGACL Test Cell Drop (0xd2000063): 0 frames
Egress IPv6 SGACL Test Cell Drop (0x40000064): 0 frames
Egress IPv4 Pre SGACL Forward (0x2c000067): 0 frames
```

show platform software fed switch active acl usage

To display SGACL usage, use the **show platform software fed switch active acl usage** command in privileged EXEC mode.

show platform software fed switch active acl usage

| Syntax Description | usage Displays ACL usage. | | | | |
|-----------------------------|---|---------|--------------|-----------------------------|------------------------------|
| Command Modes | Privileged EXEC (#) | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Everest 16.6.1</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | Cisco IOS XE Everest 16.6.1 | This command was introduced. |
| Release | Modification | | | | |
| Cisco IOS XE Everest 16.6.1 | This command was introduced. | | | | |

Example

The following is sample output from the **show platform software fed switch active acl usage** command:

```
Device# show platform software fed switch active acl usage
#####
#####
#####      Printing Usage Infos      #####
#####
#####
##### ACE Software VMR max:196608 used:282
#####
=====
Feature Type          ACL Type      Dir          Name          Entries
Used
SGACL                 IPV4          Egress       V4SGACL7100   2
=====
Feature Type          ACL Type      Dir          Name          Entries
Used
SGACL_CATCHALL       IPV4          Egress       V4SGACL8100   1
=====
Feature Type          ACL Type      Dir          Name          Entries
Used
SGACL_CATCHALL       IPV6          Egress       V6SGACL9100   1
=====
```

Output fields are self-explanatory.

show platform software fed switch active ifm mappings

show platform software fed switch active ifm mappings

| | |
|---------------------------|---|
| Syntax Description | ifm Displays interface manager information. |
| | mappings Displays interface to hardware mapping information. |

Command Modes Privileged EXEC (#)

| | | |
|------------------------|-----------------------------|------------------------------|
| Command History | Release | Modification |
| | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

Example

The following is sample output from the **show platform software fed switch active ifm mappings** command:

```
Device#show platform software fed switch active ifm mappings
```

| Interface | IF_ID | Inst | Asic | Core | Port | SubPort | Mac | Cntx | LPN | GPN | Type |
|-----------------------|-------|------|------|------|------|---------|-----|------|-----|-----|-------|
| Active | | | | | | | | | | | |
| GigabitEthernet3/0/1 | 0xa | 1 | 0 | 1 | 0 | 0 | 26 | 6 | 1 | 193 | NIF Y |
| GigabitEthernet3/0/2 | 0xb | 1 | 0 | 1 | 1 | 0 | 6 | 7 | 2 | 194 | NIF Y |
| GigabitEthernet3/0/3 | 0xc | 1 | 0 | 1 | 2 | 0 | 28 | 8 | 3 | 195 | NIF Y |
| GigabitEthernet3/0/4 | 0xd | 1 | 0 | 1 | 3 | 0 | 27 | 9 | 4 | 196 | NIF Y |
| GigabitEthernet3/0/5 | 0xe | 1 | 0 | 1 | 4 | 0 | 30 | 10 | 5 | 197 | NIF Y |
| GigabitEthernet3/0/6 | 0xf | 1 | 0 | 1 | 5 | 0 | 29 | 11 | 6 | 198 | NIF Y |
| GigabitEthernet3/0/7 | 0x10 | 1 | 0 | 1 | 6 | 0 | 32 | 12 | 7 | 199 | NIF Y |
| GigabitEthernet3/0/8 | 0x11 | 1 | 0 | 1 | 7 | 0 | 31 | 13 | 8 | 200 | NIF Y |
| GigabitEthernet3/0/9 | 0x12 | 1 | 0 | 1 | 8 | 0 | 19 | 14 | 9 | 201 | NIF Y |
| GigabitEthernet3/0/10 | 0x13 | 1 | 0 | 1 | 9 | 0 | 5 | 15 | 10 | 202 | NIF Y |
| GigabitEthernet3/0/11 | 0x14 | 1 | 0 | 1 | 10 | 0 | 21 | 16 | 11 | 203 | NIF Y |
| GigabitEthernet3/0/12 | 0x15 | 1 | 0 | 1 | 11 | 0 | 20 | 17 | 12 | 204 | NIF Y |
| GigabitEthernet3/0/13 | 0x16 | 1 | 0 | 1 | 12 | 0 | 23 | 18 | 13 | 205 | NIF Y |
| GigabitEthernet3/0/14 | 0x17 | 1 | 0 | 1 | 13 | 0 | 22 | 19 | 14 | 206 | NIF Y |
| GigabitEthernet3/0/15 | 0x18 | 1 | 0 | 1 | 14 | 0 | 25 | 20 | 15 | 207 | NIF Y |
| GigabitEthernet3/0/16 | 0x19 | 1 | 0 | 1 | 15 | 0 | 24 | 21 | 16 | 208 | NIF Y |
| GigabitEthernet3/0/17 | 0x1a | 1 | 0 | 1 | 16 | 0 | 12 | 22 | 17 | 209 | NIF Y |
| GigabitEthernet3/0/18 | 0x1b | 1 | 0 | 1 | 17 | 0 | 4 | 23 | 18 | 210 | NIF Y |
| GigabitEthernet3/0/19 | 0x1c | 1 | 0 | 1 | 18 | 0 | 14 | 24 | 19 | 211 | NIF Y |
| GigabitEthernet3/0/20 | 0x1d | 1 | 0 | 1 | 19 | 0 | 13 | 25 | 20 | 212 | NIF Y |
| GigabitEthernet3/0/21 | 0x1e | 1 | 0 | 1 | 20 | 0 | 16 | 26 | 21 | 213 | NIF Y |
| GigabitEthernet3/0/22 | 0x1f | 1 | 0 | 1 | 21 | 0 | 15 | 27 | 22 | 214 | NIF Y |
| GigabitEthernet3/0/23 | 0x20 | 1 | 0 | 1 | 22 | 0 | 18 | 28 | 23 | 215 | NIF Y |
| GigabitEthernet3/0/24 | 0x21 | 1 | 0 | 1 | 23 | 0 | 17 | 29 | 24 | 216 | NIF Y |
| GigabitEthernet3/0/25 | 0x22 | 0 | 0 | 0 | 24 | 0 | 26 | 6 | 25 | 217 | NIF Y |
| GigabitEthernet3/0/26 | 0x23 | 0 | 0 | 0 | 25 | 0 | 6 | 7 | 26 | 218 | NIF Y |
| GigabitEthernet3/0/27 | 0x24 | 0 | 0 | 0 | 26 | 0 | 28 | 8 | 27 | 219 | NIF Y |
| GigabitEthernet3/0/28 | 0x25 | 0 | 0 | 0 | 27 | 0 | 27 | 9 | 28 | 220 | NIF Y |
| GigabitEthernet3/0/29 | 0x26 | 0 | 0 | 0 | 28 | 0 | 30 | 10 | 29 | 221 | NIF Y |
| GigabitEthernet3/0/30 | 0x27 | 0 | 0 | 0 | 29 | 0 | 29 | 11 | 30 | 222 | NIF Y |
| GigabitEthernet3/0/31 | 0x28 | 0 | 0 | 0 | 30 | 0 | 32 | 12 | 31 | 223 | NIF Y |
| GigabitEthernet3/0/32 | 0x29 | 0 | 0 | 0 | 31 | 0 | 31 | 13 | 32 | 224 | NIF Y |
| GigabitEthernet3/0/33 | 0x2a | 0 | 0 | 0 | 32 | 0 | 19 | 14 | 33 | 225 | NIF Y |

```

GigabitEthernet3/0/34    0x2b    0 0 0    33    0    5    15    34    226    NIF    Y
GigabitEthernet3/0/35    0x2c    0 0 0    34    0    21    16    35    227    NIF    Y
GigabitEthernet3/0/36    0x2d    0 0 0    35    0    20    17    36    228    NIF    Y
GigabitEthernet3/0/37    0x2e    0 0 0    36    0    23    18    37    229    NIF    Y
GigabitEthernet3/0/38    0x2f    0 0 0    37    0    22    19    38    230    NIF    Y
GigabitEthernet3/0/39    0x30    0 0 0    38    0    25    20    39    231    NIF    Y
GigabitEthernet3/0/40    0x31    0 0 0    39    0    24    21    40    232    NIF    Y
GigabitEthernet3/0/41    0x32    0 0 0    40    0    12    22    41    233    NIF    Y
GigabitEthernet3/0/42    0x33    0 0 0    41    0    4    23    42    234    NIF    Y
GigabitEthernet3/0/43    0x34    0 0 0    42    0    14    24    43    235    NIF    Y
GigabitEthernet3/0/44    0x35    0 0 0    43    0    13    25    44    236    NIF    Y
GigabitEthernet3/0/45    0x36    0 0 0    44    0    16    26    45    237    NIF    Y
GigabitEthernet3/0/46    0x37    0 0 0    45    0    15    27    46    238    NIF    Y
GigabitEthernet3/0/47    0x38    0 0 0    46    0    18    28    47    239    NIF    Y
GigabitEthernet3/0/48    0xd8    0 0 0    47    0    17    29    48    240    NIF    Y
GigabitEthernet3/1/1    0x3a    1 0 1    48    0    3    4    49    241    NIF    N
GigabitEthernet3/1/2    0x3b    1 0 1    49    0    2    5    50    242    NIF    N
GigabitEthernet3/1/3    0x3c    0 0 0    50    0    3    4    51    243    NIF    N
GigabitEthernet3/1/4    0x3d    0 0 0    51    0    2    5    52    244    NIF    N
TenGigabitEthernet3/1/1  0x3e    1 0 1    52    0    3    3    53    245    NIF    N
TenGigabitEthernet3/1/2  0x3f    1 0 1    53    0    2    2    54    246    NIF    N
TenGigabitEthernet3/1/3  0x40    1 0 1    54    0    1    1    55    247    NIF    N
TenGigabitEthernet3/1/4  0x41    1 0 1    55    0    0    0    56    248    NIF    N
TenGigabitEthernet3/1/5  0x42    0 0 0    56    0    3    3    57    249    NIF    N
TenGigabitEthernet3/1/6  0x43    0 0 0    57    0    2    2    58    250    NIF    N
TenGigabitEthernet3/1/7  0x44    0 0 0    58    0    1    1    59    251    NIF    N
TenGigabitEthernet3/1/8  0x45    0 0 0    59    0    0    0    60    252    NIF    N
FortyGigabitEthernet3/1/1 0x46    1 0 1    60    0    0    0    61    253    NIF    N
FortyGigabitEthernet3/1/2 0x47    0 0 0    61    0    0    0    62    254    NIF    N
TwentyFiveGigE3/1/1    0x48    1 0 1    62    0    0    0    63    255    NIF    N
TwentyFiveGigE3/1/2    0x49    0 0 0    63    0    0    0    64    256    NIF    N
AppGigabitEthernet3/0/1  0x4a    1 0 1    24    0    11    30    65    257    NIF    Y

```

The following table explains the significant fields shown in the output:

| Field | Description |
|-----------|---|
| Interface | The name of the interface. |
| IF_ID | The interface ID. |
| Inst | The instance ID. |
| Asic | The ASIC number. |
| Core | The core number. |
| Port | The port number of the interface. |
| SubPort | The number of subports. |
| MAC | The MAC address. |
| LPN | The local port number inside ASIC. |
| GPN | The global system number inside switch. |
| Type | The type of interface. |
| Active | The interface status (active/inactive). |

show platform software fed switch active ip route

To display IP route information, use the **show platform software fed switch active ip route** command in privileged EXEC mode.

show platform software fed switch active ip route

| Syntax Description | |
|--------------------|--|
| ip | Accepts IP commands. |
| route | Displays IPv4 Forwarding Information Base (FIB) details. |

| Command Modes | |
|---------------|---------------------|
| | Privileged EXEC (#) |

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

Example

The following is sample output from the **show platform software fed switch active ip route** command:

```
Device# show platform software fed switch active ip route
vrf  dest                               htm          flags  SGT  DGID  MPLS
  Last-modified           SecsSinceHit
---  ----
-----
2    0.0.0.0/0                               0x78f2fd3488a8 0x0    0    0
  2023/03/14 06:38:18.684                1
2    127.0.0.0/8                             0x78f2fd351508 0x0    0    0
  2023/03/14 06:38:18.687                1
2    255.255.255.255/32                       0x78f2fd34ebd8 0x0    0    0
  2023/03/14 06:38:18.686                1
2    240.0.0.0/4                              0x78f2fd350828 0x0    0    0
  2023/03/14 06:38:18.686                1
2    0.0.0.0/32                              0x78f2fd34cd88 0x0    0    0
  2023/03/14 06:38:18.685                1
2    0.0.0.0/8                              0x78f2fd350e98 0x0    0    0
  2023/03/14 06:38:18.686                1
0    0.0.0.0/0                               0x78f2fd345388 0x0    0    0
  2023/03/14 06:39:09.383                352
0    9.24.0.0/32                             0x78f2fd33e1c8 0x0    0    0
  2023/03/14 06:38:38.930                1
0    9.24.0.1/32                             0x78f2fd33a5e8 0x0    0    0
  2023/03/14 06:39:09.390                5
0    127.0.0.0/8                             0x78f2fd3501b8 0x0    0    0
  2023/03/14 06:38:18.686                1
0    255.255.255.255/32                       0x78f2fd34c478 0x0    0    0
  2023/03/14 06:38:18.685                1
0    2.2.2.2/32                              0x78f2fd3568e8 0x0    2    1
  2023/03/14 06:39:09.383                1
0    9.24.255.255/32                         0x78f2fd344838 0x0    0    0
  2023/03/14 06:38:38.931                1
0    10.64.69.164/32                         0x78f2fd33fac8 0x0    0    0
  2023/03/14 06:39:09.383                1
0    10.77.128.69/32                         0x78f2fd3420a8 0x0    0    0
```



```

2023/03/14 06:39:09.383          1
0      240.0.0.0/4                0x78f2fd34f4d8 0x0      0      0
2023/03/14 06:38:18.686          1
0      10.106.26.249/32           0x78f2fd3399a8 0x0      0      0
2023/03/14 06:39:09.383          1
0      0.0.0.0/32                  0x78f2fd34a768 0x0      0      0
2023/03/14 06:38:18.685          1
0      9.24.23.30/32              0x78f2fd1f2078 0x0      0      0
2023/03/14 06:38:38.930         24
0      9.24.0.0/16                 0x78f2fd33af48 0x0      0      0
2023/03/14 06:38:38.930          1
0      0.0.0.0/8                   0x78f2fd34fb48 0x0      0      0
2023/03/14 06:38:18.686          1

```

The following table explains the significant fields shown in the output:

| Field | Description |
|-------|---|
| vrf | The VRF ID. |
| dest | The destination address. |
| htm | The hash table manager object pointer for IP route. |
| SGT | The security group tag. |
| DGID | The destination tag ID. |

show platform software fed switch active sgacl detail

To display global enforcement status along with policy and count information, use the **show platform software fed switch active sgacl detail** command in privileged EXEC mode.

show platform software fed switch active sgacl detail

| Syntax Description | |
|--------------------|--------------------------------------|
| sgacl | Displays SGACL hardware information. |
| detail | Displays detailed SGACL information. |

| Command Modes | |
|---------------|---------------------|
| | Privileged EXEC (#) |

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

Example

The following is sample output from the **show platform software fed switch active sgacl detail** command:

```
Device# show platform software fed switch active sgacl detail
Global Enforcement: Off

*Refcnt: for the non-SGACL feature
===== DGID Table =====
SGT/Refcnt      DGT      DGID      test_cell monitor  permitted  denied
=====
*/3             2        1
```

The following table explains the significant fields shown in the output:

| Field | Description |
|------------|---------------------------------------|
| SGT/Refcnt | The security group tag/reinforcement. |
| DGT | The destination tag. |
| DGID | The destination tag ID. |

show platform software fed switch active sgacl port

To display Layer 2 interface configuration settings for all interfaces, use the **show platform software fed switch active sgacl port** command in privileged EXEC mode.

show platform software fed switch active sgacl port

| Syntax Description | |
|--------------------|--------------------------------------|
| sgacl | Displays SGACL hardware information. |
| port | Specifies port configuration. |

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

Example

The following is sample output from the **show platform software fed switch active sgacl port** command:

```
Device# show platform software fed switch active sgacl port
```

| Port | Status | Port-SGT | Trust | Propagate | IngressCache | EgressCache |
|----------|----------|----------|-------|-----------|--------------|-------------|
| Gi3/0/1 | Disabled | 0 | No | No | No | No |
| Gi3/0/2 | Disabled | 0 | No | No | No | No |
| Gi3/0/3 | Disabled | 0 | No | No | No | No |
| Gi3/0/4 | Disabled | 0 | No | No | No | No |
| Gi3/0/5 | Disabled | 0 | No | No | No | No |
| Gi3/0/6 | Disabled | 0 | No | No | No | No |
| Gi3/0/7 | Disabled | 0 | No | No | No | No |
| Gi3/0/8 | Disabled | 0 | No | No | No | No |
| Gi3/0/9 | Disabled | 0 | No | No | No | No |
| Gi3/0/10 | Disabled | 0 | No | No | No | No |
| Gi3/0/11 | Disabled | 0 | No | No | No | No |
| Gi3/0/12 | Disabled | 0 | No | No | No | No |
| Gi3/0/13 | Disabled | 0 | No | No | No | No |
| Gi3/0/14 | Disabled | 0 | No | No | No | No |
| Gi3/0/15 | Disabled | 0 | No | No | No | No |
| Gi3/0/16 | Disabled | 0 | No | No | No | No |
| Gi3/0/17 | Disabled | 0 | No | No | No | No |
| Gi3/0/18 | Disabled | 0 | No | No | No | No |
| Gi3/0/19 | Disabled | 0 | No | No | No | No |
| Gi3/0/20 | Disabled | 0 | No | No | No | No |
| Gi3/0/21 | Disabled | 0 | No | No | No | No |
| Gi3/0/22 | Disabled | 0 | No | No | No | No |
| Gi3/0/23 | Disabled | 0 | No | No | No | No |
| Gi3/0/24 | Disabled | 0 | No | No | No | No |
| Gi3/0/25 | Disabled | 0 | No | No | No | No |
| Gi3/0/26 | Disabled | 0 | No | No | No | No |
| Gi3/0/27 | Disabled | 0 | No | No | No | No |
| Gi3/0/28 | Disabled | 0 | No | No | No | No |
| Gi3/0/29 | Disabled | 0 | No | No | No | No |
| Gi3/0/30 | Disabled | 0 | No | No | No | No |
| Gi3/0/31 | Disabled | 0 | No | No | No | No |
| Gi3/0/32 | Disabled | 0 | No | No | No | No |

show platform software fed switch active sgACL port

| | | | | | | |
|----------|----------|---|----|----|----|----|
| Gi3/0/33 | Disabled | 0 | No | No | No | No |
| Gi3/0/34 | Disabled | 0 | No | No | No | No |
| Gi3/0/35 | Disabled | 0 | No | No | No | No |
| Gi3/0/36 | Disabled | 0 | No | No | No | No |
| Gi3/0/37 | Disabled | 0 | No | No | No | No |
| Gi3/0/38 | Disabled | 0 | No | No | No | No |
| Gi3/0/39 | Disabled | 0 | No | No | No | No |
| Gi3/0/40 | Disabled | 0 | No | No | No | No |
| Gi3/0/41 | Disabled | 0 | No | No | No | No |
| Gi3/0/42 | Disabled | 0 | No | No | No | No |
| Gi3/0/43 | Disabled | 0 | No | No | No | No |
| Gi3/0/44 | Disabled | 0 | No | No | No | No |
| Gi3/0/45 | Disabled | 0 | No | No | No | No |
| Gi3/0/46 | Disabled | 0 | No | No | No | No |
| Gi3/0/47 | Disabled | 0 | No | No | No | No |
| Gi3/0/48 | Disabled | 0 | No | No | No | No |
| Gi3/1/1 | Disabled | 0 | No | No | No | No |
| Gi3/1/2 | Disabled | 0 | No | No | No | No |
| Gi3/1/3 | Disabled | 0 | No | No | No | No |
| Gi3/1/4 | Disabled | 0 | No | No | No | No |
| Te3/1/1 | Disabled | 0 | No | No | No | No |
| Te3/1/2 | Disabled | 0 | No | No | No | No |
| Te3/1/3 | Disabled | 0 | No | No | No | No |
| Te3/1/4 | Disabled | 0 | No | No | No | No |
| Te3/1/5 | Disabled | 0 | No | No | No | No |
| Te3/1/6 | Disabled | 0 | No | No | No | No |
| Te3/1/7 | Disabled | 0 | No | No | No | No |
| Te3/1/8 | Disabled | 0 | No | No | No | No |
| Fo3/1/1 | Disabled | 0 | No | No | No | No |
| Fo3/1/2 | Disabled | 0 | No | No | No | No |
| Tw3/1/1 | Disabled | 0 | No | No | No | No |
| Tw3/1/2 | Disabled | 0 | No | No | No | No |
| Ap3/0/1 | Disabled | 0 | No | No | No | No |

Output fields are self-explanatory.

show platform software fed switch active sgacl vlan

To display global enforcement status on VLANs, use the **show platform software fed switch active sgacl vlan** command in privileged EXEC mode.

show platform software fed switch active sgacl vlan

Syntax Description

sgacl Displays SGACL hardware information.

vlan Specifies VLAN configuration.

Command Modes

Privileged EXEC (#)

Command History

Release

Modification

Cisco IOS XE Everest 16.6.1

This command was introduced.

Example

The following is sample output from the **show platform software fed switch active sgacl vlan** command:

```
Device# show platform software fed switch active sgacl vlan
```

```
Enforcement enabled:  
vlan0  
vlan1  
vlan2  
vlan10  
vlan102  
vlan192  
vlan200
```

show platform software status control-processor brief

To display brief information about CPU and memory, use the **show platform software status control-processor brief** command in privileged EXEC mode.

show platform software status control-processor brief

| Syntax Description | status | Displays system status. |
|--------------------|--------------------------|------------------------------------|
| | control-processor | Displays control processor status. |
| | brief | Displays brief status. |

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-----------------------------|------------------------------|
| | Cisco IOS XE Everest 16.6.1 | This command was introduced. |

Example

The following is sample output from the **show platform software status control-processor brief** command:

```
Device# show platform software status control-processor brief
```

```
Load Average
```

```
Slot Status 1-Min 5-Min 15-Min
3-RP0 Healthy 0.03 0.07 0.04
```

```
Memory (kB)
```

```
Slot Status Total Used (Pct) Free (Pct) Committed (Pct)
3-RP0 Healthy 7745656 4178292 (54%) 3567364 (46%) 4755060 (61%)
```

```
CPU Utilization
```

```
Slot CPU User System Nice Idle IRQ SIRQ IOwait
3-RP0 0 0.50 0.40 0.00 99.10 0.00 0.00 0.00
      1 0.90 0.50 0.00 98.59 0.00 0.00 0.00
      2 0.40 0.40 0.00 99.20 0.00 0.00 0.00
      3 0.80 0.30 0.00 98.90 0.00 0.00 0.00
      4 0.60 0.30 0.00 99.09 0.00 0.00 0.00
      5 0.70 0.30 0.00 99.00 0.00 0.00 0.00
      6 1.20 0.30 0.00 98.50 0.00 0.00 0.00
      7 0.59 0.39 0.00 99.00 0.00 0.00 0.00
```

Output fields are self-explanatory.